under this section may collect from a beneficiary a monthly fee for expenses (including overhead) it has incurred in providing payee services to a beneficiary. The limit on the fee a qualified organization may collect for providing payee services increases by the same percentage as the annual cost of living adjustment (COLA). The increased fee amount (rounded to the nearest dollar) is taken beginning with the payment for January.

(2) Any agreement providing for a fee in excess of the amount permitted shall be void and treated as misuse of your benefits by the organization under § 416.641.

(3) A fee may be collected for any month during which the organization—

(i) Provides representative payee services;

(ii) Receives a benefit payment for the beneficiary; and

(iii) Is authorized to receive a fee for representative payee services.

(4) Fees for services may not be taken from any funds conserved for the beneficiary by a payee in accordance with § 416.645.

(5) Generally, an organization may not collect a fee for months in which it does not receive a benefit payment. However, an organization will be allowed to collect a fee for months in which it did not receive a payment if we later issue payment for these months and the organization:

(i) Received our approval to collect a fee for the months for which payment is made;

(ii) Provided payee services in the months for which payment is made; and

(iii) Was the payee when the retroactive payment was paid by us.

(6) An authorized organization can collect a fee for providing representative payee services from another source if the total amount of the fee collected from both the beneficiary and the other source does not exceed the amount authorized by us.

23. Revise § 416.641 to read as follows:

§ 416.641 Who is liable if your representative payee misuses your benefits?

(a) A representative payee who misuses your benefits is responsible for paying back misused benefits. We will make every reasonable effort to obtain restitution of misused benefits so that these benefits can be repaid to you.

(b) We will repay benefits in cases when we determine that a representative payee misused benefits and we were negligent in the investigation or monitoring of that representative payee. When we make restitution, we will pay you or your alternative representative payee an amount equal to the misused benefits less any amount repaid by the misuser.

(c) The term ''negligent failure'' used in this subpart means that we failed to investigate or monitor a representative payee or that we did investigate or monitor a representative payee but did not follow established procedures in our investigation or monitoring. Examples of our negligent failure include, but are not limited to, the following:

(1) We did not follow our established procedures in this subpart when investigating, appointing, or monitoring a representative payee;

(2) We did not investigate timely a reported allegation of misuse; or

(3) We did not take the steps necessary to prevent the issuance of payments to the representative payee after it was determined that the payee misused benefits.

(d) Our repayment of misused benefits under these provisions does not alter the representative payee's liability and responsibility as described in paragraph (a) of this section.

24. Revise § 416.650 to read as follows:

§ 416.650 When will we select a new representative payee for you?

When we learn that your interest is not served by sending your benefit payment to your present representative payee or that your present payee is no longer able or willing to carry out payee responsibilities, we will promptly stop sending your payment to the payee. We will then send your benefit payment to an alternative payee or directly to you, until we find a suitable payee. We may suspend payment as explained in § 416.611(c) if we find that paying you directly would cause substantial harm and we cannot find a suitable alternative representative payee before your next payment is due. We will terminate payment of benefits to your representative payee and find a new payee or pay you directly if the present payee:

(a) Has been found by us or a court of competent jurisdiction to have misused your benefits;

(b) Has not used the benefit payments on your behalf in accordance with the guidelines in this subpart;

(c) Has not carried out the other responsibilities described in this subpart;

(d) Dies;

(e) No longer wishes to be your payee;

(f) Is unable to manage your benefit payments; or

(g) Fails to cooperate, within a reasonable time, in providing evidence, accounting, or other information we request.

25. Revise § 416.665 to read as follows:

§ 416.665 How does your representative payee account for the use of benefits?

A representative payee must account for the use of benefits. We require written reports from your representative payee no less than annually (except for certain State institutions which participate in a separate onsite review program). We may verify how your representative payee used the funds. Your representative payee should keep records of how benefits were used in order to make accounting reports and make those records available upon our request. We may ask your representative payee to give us the following information:

(a) Where you lived during the accounting period;

(b) Who made the decisions on how your benefits were spent or saved;

(c) How your benefit payments were used; and

(d) How much of your benefit payments were saved and how the savings were invested.

26. The authority citation for subpart N continues to read as follows:

Authority: Secs. 702(a)(5), 1631, and 1633 of the Social Security Act (42 U.S.C. 902(a)(5), 1383, and 1383(b)); 31 U.S.C. 3720A.

27. Amend § 416.1402 by revising paragraph (d), removing the word ''and'' at the end of paragraph (m), replacing the period at the end of paragraph (n) with ''; and,'' and adding paragraph (o) to read as follows:

§ 416.1402 Administrative actions that are initial determinations.

* * * * *

(d) Whether the payment of your benefits will be made, on your behalf, to a representative payee;

* * * * *

(o) Whether we were negligent in failing to investigate or monitor your representative payee, which resulted in the misuse of benefits by your representative payee.

[FR Doc. 03–24017 Filed 9–24–03; 8:45 am]

BILLING CODE 4191–02–P

DEPARTMENT OF THE TREASURY

31 CFR Part 103

RIN 1506–AA28

Customer Identification Programs for Financial Institutions

AGENCY: Departmental Offices, Treasury.

ACTION: Disposition of comments and termination of inquiry.

SUMMARY: The Department of the Treasury is announcing the results of its July 1, 2003, Notice of Inquiry that sought comment on two aspects of the final rules issued pursuant to section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (the Act). Following a review of comments and a careful analysis of the issues, Treasury has determined that no changes to the final rules are warranted.

FOR FURTHER INFORMATION CONTACT: Office of the General Counsel, (202) 622–1927.

SUPPLEMENTARY INFORMATION:

I. Background

On May 9, 2003, the Department of the Treasury (Treasury), through the Financial Crimes Enforcement Network (FinCEN), together with the federal functional regulators, jointly issued final rules implementing section 326 of the Act.[1] The final rules require banks, securities broker-dealers, mutual funds, and futures commission merchants and introducing brokers to establish reasonable procedures for the identification and verification of new accountholders. These rules became effective on June 9, 2003, although financial institutions have until October 1, 2003 to come into compliance.

On July 1, 2003, Treasury published a Notice of Inquiry seeking additional comment on two discrete aspects of the final rules: (i) Whether and under what circumstances financial institutions should be required to retain photocopies of identification documents relied on to verify customer identity; and (ii) whether there are situations when the regulations should preclude reliance on certain forms of foreign government-issued identification to verify customer identity.[2]

II. Summary of Comments

Treasury received over 34,000 comments in response to the Notice of Inquiry.[3] All comments have been reviewed. Treasury received comments from a wide variety of individuals and entities, including members of Congress, the Department of Justice, representatives and officials of State and local governments, the financial services industry (including the banking, securities, mutual fund, and insurance industries), faith-based organizations, advocacy groups, and interested citizens.

The Photocopy Issue: Treasury received approximately 10,700 comments relating to the question of whether the final rules should require financial institutions to make and retain photocopies of identification documents relied upon to verify identity. As issued, the final regulations do not require financial institutions to photocopy identification documents. Although it is not dispositive of the issue, Treasury notes that the great majority of those submitting comments, nearly 90 percent, did not believe that the rules should be amended to require financial institutions to make and retain photocopies of identification documents.

The Foreign Identification Documents Issue: Treasury received approximately 24,000 comments relating to the question of whether the final rules should preclude financial institutions from relying on certain forms of identification issued by a foreign government. As issued, the final rules neither endorse nor preclude reliance on particular forms of foreign government issued identification. Virtually all comments were directed toward encouraging Treasury either to allow financial institutions to accept, or to preclude them from accepting, the Mexican consular identification document, the Matricula Consular. Indeed, many of the comments addressed questions of immigration policy, rather than the security of such documents. Again, although not dispositive of the issue, the vast majority of those submitting comments, nearly 83 percent, did not believe that the final rules should be changed to preclude reliance on certain forms of identification issued by a foreign government.

III. Resolution

Treasury issued the Notice of Inquiry to enhance the administrative record with respect to the two issues outlined above. The addition of over 34,000 comments has done precisely that. Despite the volume of comments received, the comments presented no new arguments or information relative to the requirements of the final rules that Treasury and the financial regulators did not already consider in developing the final rules.

Treasury remains persuaded, as it was at the conclusion of the rulemaking process, that requiring photocopies of identification documents is not an appropriate requirement to impose. While individual financial institutions may well determine that it is prudent to photocopy identification documents in some instances, an across-the-board requirement is inconsistent with the risk-based approach of the final rules and is not warranted.

The divergence of opinion concerning the relative security of consular identification cards demonstrates the difficulties associated with drafting a rule that would purport to specify ''unacceptable'' documents. And, given the wide array of identity documents available, the security and reliability of which is constantly changing, it makes little sense from a regulatory perspective to specify individual types of documents that cannot be used within the regulation itself. Any such list would inevitably be quickly out of date and may provide financial institutions with an unwarranted sense of security about documents that are not prohibited. Treasury is committed to protecting the financial system from abuse by those seeking to finance terrorism or commit financial crimes. This commitment includes providing financial institutions with information relating to the security and reliability of identification cards. Treasury will use appropriate methods, both formal and informal, to ensure that such information is collected and shared with the financial community to assist them in verifying the identity of their customers.

IV. Compliance Deadline

Numerous commenters from the financial community requested that Treasury extend the October 1, 2003 deadline for complying with the customer identification regulations in light of the Notice of Inquiry. The implementation deadline will not be extended. Treasury expects all financial institutions covered by the customer identification regulations to have their customer identification program drafted and approved by October 1, 2003.

[1] *See* 68 FR 25089–25162. The Federal functional regulators include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. In addition to the joint rules, FinCEN also issued separately a rule applicable to various state chartered institutions lacking a Federal functional regulator.

[2] 68 FR 39039.

[3] Treasury received over 27,000 comment letters, e-mails, and web postings. Many of the comment letters offered separate opinions on the two issues, thus raising the total number of comments received on the two issues to over 34,000.

Dated: September 17, 2003.

Wayne A. Abernathy,

Assistant Secretary of the Treasury.

[FR Doc. 03–24226 Filed 9–24–03; 8:45 am]

BILLING CODE 4810–25–P

DEPARTMENT OF DEFENSE

Department of the Air Force

32 CFR Part 806b

[Air Force Instruction 33–332]

Privacy Act; Implementation

AGENCY: Department of the Air Force, DoD.

ACTION: Proposed rule.

SUMMARY: The Department of the Air Force proposes to revise the Privacy Act Program Instruction. The revision moves responsibility for the Air Force Privacy Program from AFCIC to AF–CIO; prescribes AFVA 33–276, Privacy Act Label as optional; adds the E-Gov Act of 2002 requirement for a Privacy Impact Assessment for all information systems that are new or have major changes; changes appeal processing from AFCIC to Air Force Legal Services Agency (AFLSA/JACL); adds Privacy Act warning language to use on information systems subject to the Privacy Act, includes guidance on sending personal information via e-mail; adds procedures on complaints; and provides guidance on recall rosters; social rosters; consent statements, systems of records operated by a contractor, and placing information on shared drives.

DATES: Submit comments on or before October 27, 2003.

ADDRESSES: Address all comments concerning this proposed rule to Mrs. Anne Rollins, Office of the Air Force Chief Information Officer, AF–CIO/P, 1155 Air Force Pentagon, Washington, DC 20330–1155.

FOR FURTHER INFORMATION CONTACT: Mrs. Anne Rollins, 703–601–4043.

SUPPLEMENTARY INFORMATION:

List of Subjects in 32 CFR Part 806b

Privacy.

For the reasons set forth in the preamble, the Department of the Air Force is revising 32 CFR part 806b as follows:

PART 806b—PRIVACY ACT PROGRAM

Authority: 5 U.S.C. 552a.

Subpart A—Overview of the Privacy Act Program

§ 806b.1 Summary of Revisions.

This part moves responsibility for the Air Force Privacy Program from AFCIC to AF–CIO; prescribes AFVA 33–276, Privacy Act Label as optional; adds the E-Gov Act of 2002 requirement for a Privacy Impact Assessment for all information systems that are new or have major changes; changes appeal processing from AFCIC to Air Force Legal Services Agency (AFLSA/JACL); adds Privacy Act warning language to use on information systems subject to the Privacy Act, includes guidance on sending personal information via e-mail; adds procedures on complaints; and provides guidance on recall rosters; social rosters; consent statements, systems of records operated by a contractor, and placing information on shared drives.

§ 806b.2 Basic Guidelines.

This part implements the Privacy Act of 1974 and applies to records on living U.S. citizens and permanent resident aliens that are retrieved by name or personal identifier. This part also provides guidance on collecting and disseminating personal information in general.